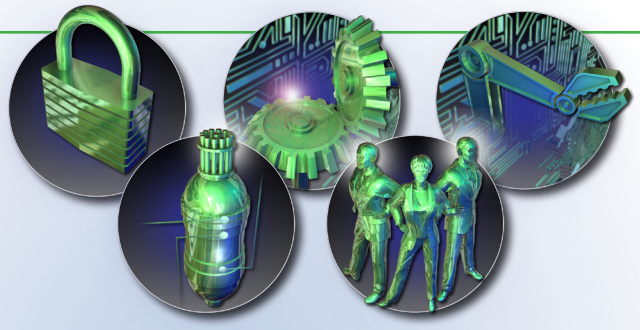
Solutions for today – vision for tomorrow



ICIS research covers five areas: Safeguards and control systems security, sensors, intelligent automation, human-systems integration, and robotics/intelligent systems

ICIS research is centered on developing components, programs, systems and individuals for any application that requires monitoring, control, and human interaction. External peer review and advisory committees made up of academic, R&D and customer organizations provide independent and ongoing review of the strategy within the signature and the focus or research funds. This research covers the five technological areas mentioned, which are further defined:

- Safeguards and control system security: Methods to protect digital systems and special nuclear material from the intelligent adversary;
- Sensors: Specialized sensors and sensing systems that are designed to monitor critical infrastructure and withstand demanding environments, such as needed for in-pile testing of advanced fuels and materials proposed for existing and next-generation nuclear power plants;
- Intelligent automation: On-line condition monitoring and prognostics, observational platform design, and advanced supervisory and predictive controls for reliable, efficient and safe operation of industrial and nuclear facilities;
- Human-systems integration: Research to advance human-centered design and operation of complex systems, considering the human interaction with the process in its various forms, including visual, audible and touch;
- Robotics and intelligent systems: Integrating sensor technology, resilient control systems, intelligent automation and human-systems design for advanced robotic applications.

Expertise

ICIS hosts a multidisciplinary team of more than 50 scientists and engineers who specialize in each technological area. Basic and applied research is performed in support of the three research mission areas, and practical design performed in support of the operating facilities. Each activity is important to the overall ICIS capability, and provides not only an individual programmatic capability but also a diverse INL capability to meet the challenges of this evolving technological area.

Facilities

ICIS has a range of research facilities and test beds dedicated to sensors, control and intelligent systems research. The laboratory offers a variety of test beds for control system research, which can be utilized for complex evaluation of control system designs for cyber security, advanced control and operational verification and validation. Sensor test beds provide a unique capability for meeting both the evolving physical security needs of our society and the next generation of reactor designs. ICIS has several robotics test beds, which provide research in industrial robotics and intelligent designs

Continued next page

Instrumentation Control & Intelligent Systems

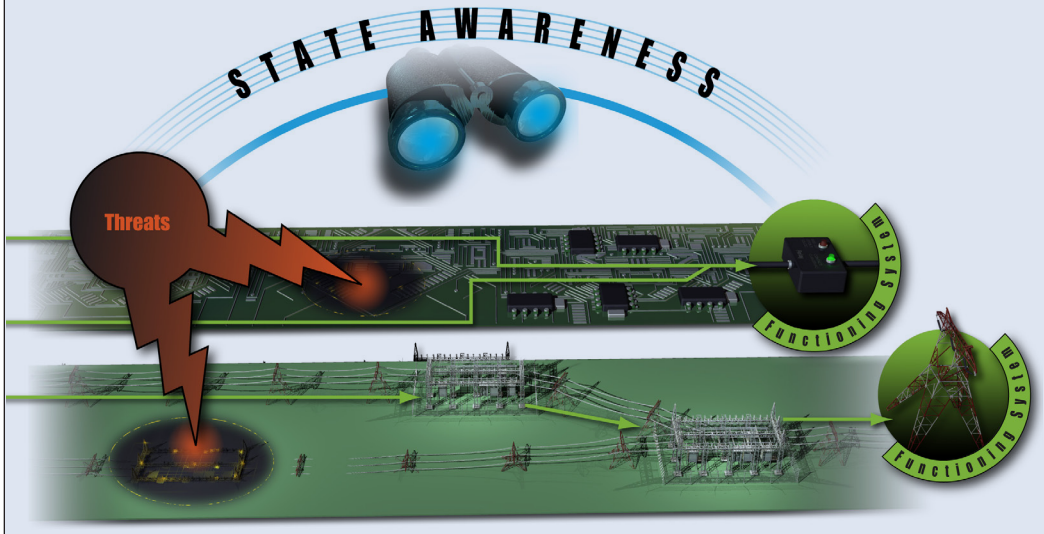
Continued from previous page

for the military and government authorities. This core capability extends to unmanned air vehicles (UAV) designs, where designers have access to an isolated airfield with full radio spectrum authority and authorization from the Federal Aviation Administration, allowing UAV operation. Because of the complexity of control system designs and the sheer level of information, advanced computing facilities support 3D human factors design for prioritized and efficient interfaces to nuclear facilities.

Grand Challenge in Resilient Control Systems

A preeminent objective for corporate and government organizations is state awareness, a comprehensive understanding of security and safety, for critical infrastructures. Given the dependence of critical infrastructure on control systems for automation, the integrity of these systems will require state awareness in order to maintain a level of public acceptability. Operators as well as government are therefore burdened to ensure they have a timely understanding of the status of their plant or all plants, respectively, to ensure efficient operations and public protection. This characterization is a significant objective that must consider many aspects of instrumentation, control, and intelligent systems in order to achieve the required result. These aspects include the control theory, intelligent systems, and human system interfaces necessary to achieve fusion of data and presentation of results that will provide an understanding of what issues are important and why.

Coupled with the need for state awareness is resilient design, which necessitates a paradigm shift with respect to the methods used in control system design. Traditional trust relationships in peer communications are no longer satisfactory since they ignore the malicious actor or actions. While fundamental principles can be applied to achieve a level of success in preventing security events, the basis of resilient design requires application of concepts of redundancy, diversity, and defense in depth to all threats and measures by which we determine proper operation. These measures, which can be categorized as cyber and physical security, process efficiency/stability, and safeguards/nonproliferation, provide the operating requirements that are monitored for state awareness and definition of the state space that needs to be considered in resilient design. The move from reactive to proactive control of plants and mechanisms by which the evaluation and verification of designs is considered all the way from design through implementation stages of resilient control systems is enabled by this paradigm shift.



A Resilient Control System maintains state awareness of process and application faults and provides the appropriate response, maintaining the desired level of system operability despite threats.

For more information

Technical Contact:

Craig Rieger
(208) 526-4136
Craig.Rieger@inl.gov

www.inl.gov/icis

A U.S. Department of Energy National Laboratory